



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
| 09/752,668 | 12/28/2000 | Dong-Gook Park | 51876p225 | 9385 |

8791 7590 01/13/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER

LIPMAN, JACOB

| | |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 01/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/752,668

Applicant(s)

PARK ET AL.

Examiner

Jacob Lipman

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-5 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-5 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Specification

1. Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1 and 2 are rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: Describing what is done with the random number selected by the client in step B of claim 1. This number is not referred

Art Unit: 2134

to later, and seems to never be checked. No weight is being given to this limitation in this office action.

4. Claim 3 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 3 recites the limitation " $x=(g^a)^{Ra+Rb}$ ". Rb has not been defined, thus leaving the function unclear.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by Curry et al., US Patent number 5,748,740.

With regard to claims 1 and 4, Curry discloses a method including the steps of, a server (module) generating a random number when a client (service provider) requests it (column 1 lines 44-51) and sending the client the random number (column 1 lines 48-51), receiving a ciphertext from the client produced using the random number and a public key of the server (column 1 lines 51-55), recovering the random number from the client and comparing it with the one sent (column 1 lines 55-59), and providing service if the numbers match (column 1 lines 59-63).

8. Claim 4 is rejected under 35 U.S.C. 102(b) as being anticipated by Schneier in Applied Cryptography.

With regard to claim 4, Schneier discloses a method including the steps of, a server (host) generating a random number when a client (Alice) requests service (page 54, paragraph 4, step 1) and sending the client the random number (step 2), receiving a ciphertext from the client produced using the random number and a random number of the client (step 3), recovering the random number from the client and comparing it with the one sent (step 4), and providing service if the numbers match (step 5).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

10. Claims 2, 3, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache, US Patent number 5,910,989 in view of Curry.

With regard to claim 2, Curry discloses the method of claim 1, but does not disclose that random numbers can be created by hashing a secret key and an index parameter. Naccache discloses that generating a random number by hashing a key and index parameter (column 5 line 62-column 6 line 4). It would have been obvious to one of ordinary skill in the art that to use the random number of Naccache in a challenge response system in order to verify a client with little processing.

With regard to claims 3, and 5, the examiner takes official notice that using exponentials is a common way to encrypt or decrypt a ciphertext, such as in Naccache (column 9). It would have been obvious for one of ordinary skill in the art to use inverse functions in Curry's system in order to verify a client with little server processing.

11. Claims 3, and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Naccache, US Patent number 5,910,989 in view of Schneier.

With regard to claims 3, and 5, the examiner takes official notice that using exponentials is a common way to encrypt or decrypt a ciphertext, such as in Naccache (column 9). It would have been obvious for one of ordinary skill in the art to use inverse functions in Schneier 's system in order to verify a client with little server processing.

12. Claims 1-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over Juels, et al, in "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks."

With regard to claims 1-5 Juels discloses the method of blocking a denial of service attack by sending a puzzle from the server to the client, where the client must return the correct solution in order to gain access to the system. Juels does not mention the random number puzzles in the claims specifically. The examiner takes official notice that inverse functions and hashing are well known in the art. It would have been obvious to one of ordinary skill in the art that inverse functions on a hashed key would be possible puzzles in Juels' method.

Response to Arguments

Art Unit: 2134

13. Applicant's arguments filed 9/27/2004 have been fully considered but they are not persuasive.

With regard to applicant's argument that claim 4 is a similar method to claim 1, the examiner points out that amended claim 1 is very different from claim 4. The examiner changed the rejection of claim 1 to Curry due to applicant's amendment to include a public key of the server in claim 1. Claim 4 was not amended to add this limitation, and thus the rejection stands.

With regard to applicant's argument that Naccache merely hashes a random number but does not produce one, the examiner points that an equation with a random number in it will always yield a random result.

With regard to applicant's argument that there is no motivation to use known functions to generate random numbers, the examiner points out that the numbers must be created. Any well-known method of creating a random number would be obvious to use in Schneier, based on the method's merits.

With regard to applicants request to show that hashing and exponents are well known puzzles, the examiner points to Raike, US Patent number 5,799,088 (column 14) who discloses a similar function to that of claims 3 and 5.

Conclusion

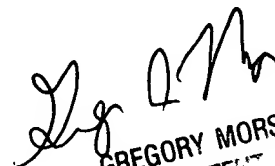
14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jacob Lipman whose telephone number is 571-272-3738. The examiner can normally be reached on 7:00 - 4:00 (M-Th).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER

Application/Control Number: 09/752,668
Art Unit: 2134

Page 8

JL